

To: Los Angeles From: Los Angeles
Re: [redacted] 02/22/2001

b3
b6
b7C
b7E

interview of the cooperating subject was handled by SA [redacted]
[redacted] from WFO and uploaded to his case file, [redacted]
[redacted] WFO is also in the process of receiving FBIHQ approval
for extraterritorial contact via the Internet. The intention, is
to use [redacted]
[redacted]

On 2/17/2001 a second prosecutive report on [redacted]
[redacted] was submitted to the AUSA's office, as requested by AUSAs
[redacted] to secure indictment of [redacted]
[redacted] The AUSAs indicated that an indictment of [redacted] should
occur within four to six weeks.

b6
b7C

Analysis of the evidence collected from [redacted]
[redacted] and from [redacted] has begun in Los Angeles,
FBIHQ Special Technologies Application Unit (STAU) and Seattle.

b6
b7C
b7E

Additional victims have been identified from the
analysis of collected evidence as well as through victim
complaints. The most recent victim identified in Los Angeles
Division is Nara Bank. The Jester group gained access to 18,000
online bank accounts and had full access to the Nara Bank
computer network.

Given the continued identification of victims and the
growing loss amount to U.S. companies, FBIHQ has decided to [redacted]
[redacted]

b7D
b7E

Los Angeles Division is currently focusing on bring
charges against [redacted] and a recently
identified target, [redacted]

b6
b7C

Investigation continuing in Los Angeles.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/22/2001

To: Los Angeles

From: Los Angeles

Squad 3/Santa Ana RA

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED] (Pending)

Title: UNSUB(S). aka

[REDACTED]
STERLING MICROSYSTEMS - VICTIM;
INTRUSION - INFO SYSTEMS;
OO: LOS ANGELES

Uplead

[Handwritten mark]

Synopsis: To update case file.

Details: On January 24-27, 2001 a conference regarding the captioned case was held at FBIHQ. In attendance were the case agents from [REDACTED] different field offices with cases opened against [REDACTED]

During the conference the depth of the investigation became known. Source information has indicated that [REDACTED] "Jester Group." The Jester group is a collection of Russian and Eastern European hackers backed by Russian Organized Crime, who break into computer networks to steal credit card and merchant accounts. The information stolen is then used to make credit card purchases or in other fraudulent schemes. Source information indicates that [REDACTED]

FBIHQ has set up a central repository for information and analysis of evidence inside of Special Investigation Operations Center (SIOC). The team managing the inflow of information and evidence are analysts from FBIHQ's Computer Investigations Unit (CIU) and Russian Organized Crime Unit.

Upon return from the captioned conference writer traveled to St. Louis Division to take part in the proffer session of a cooperating subject. The documentation of the

b3
b6
b7C
b7E

b6
b7C
b7E

b7D

b3
b7E